

CPNI

Centre for the Protection
of National Infrastructure



Token and Reader Procurement Guide

PUBLISH DATE:
June 2020

CLASSIFICATION:
Official

Token and Reader Procurement Guide

Version 2.0

Disclaimer

The information contained in this document is accurate as at the date it was created. It is intended as general guidance only and you should not rely on it. This information should be adapted for use in the specific circumstances required and you should seek specialist independent professional advice where appropriate before taking any action based on it. To the fullest extent permitted by law, CPNI accept no liability whatsoever for any loss or damage incurred or arising as a result of any error or omission in the guidance or arising from any person acting, relying upon or otherwise using the guidance. Full terms and conditions governing the use of this guidance are available on our website at www.cpni.gov.uk.

Freedom of Information Act (FOIA)

This information is supplied in confidence to the named reader and may not be disclosed further without prior approval from CPNI. This information is exempt from disclosure under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation.

Introduction

This document has been produced by CPNI to give guidance suggesting a list of key security principles to be considered when procuring Radio-Frequency Identification (RFID) smartcards and readers for Automatic Access Control Systems (AACS). It is written as advice for areas of HMG, the Critical National Infrastructure (CNI), their agencies and suppliers.

About AACS

An Automatic Access Control System is an electronic system controlling entry into and exit from a specified area.

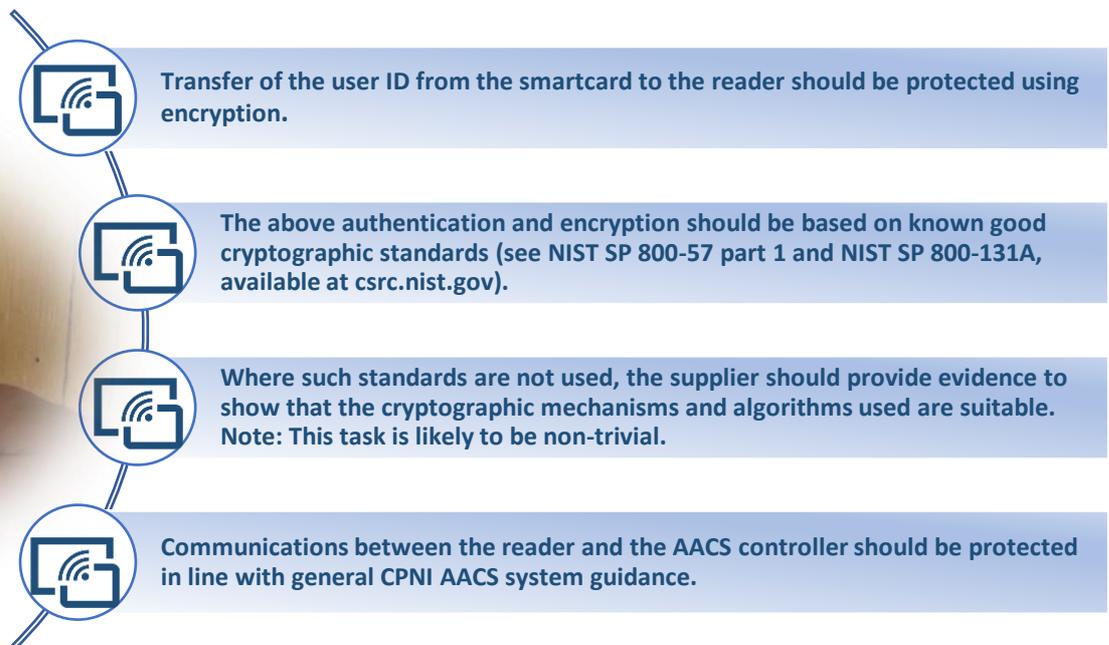
Smartcards securely store a secret unique user ID which is transferred to a reader over a secured RFID communications link. The reader then delivers the user ID which when combined with a separate typed-in user PIN provides authentication to the AACS combiner.

Key Security Principals

The following security principles should be considered when procuring AACS comprising of smartcards, (or tokens), readers and keypads.

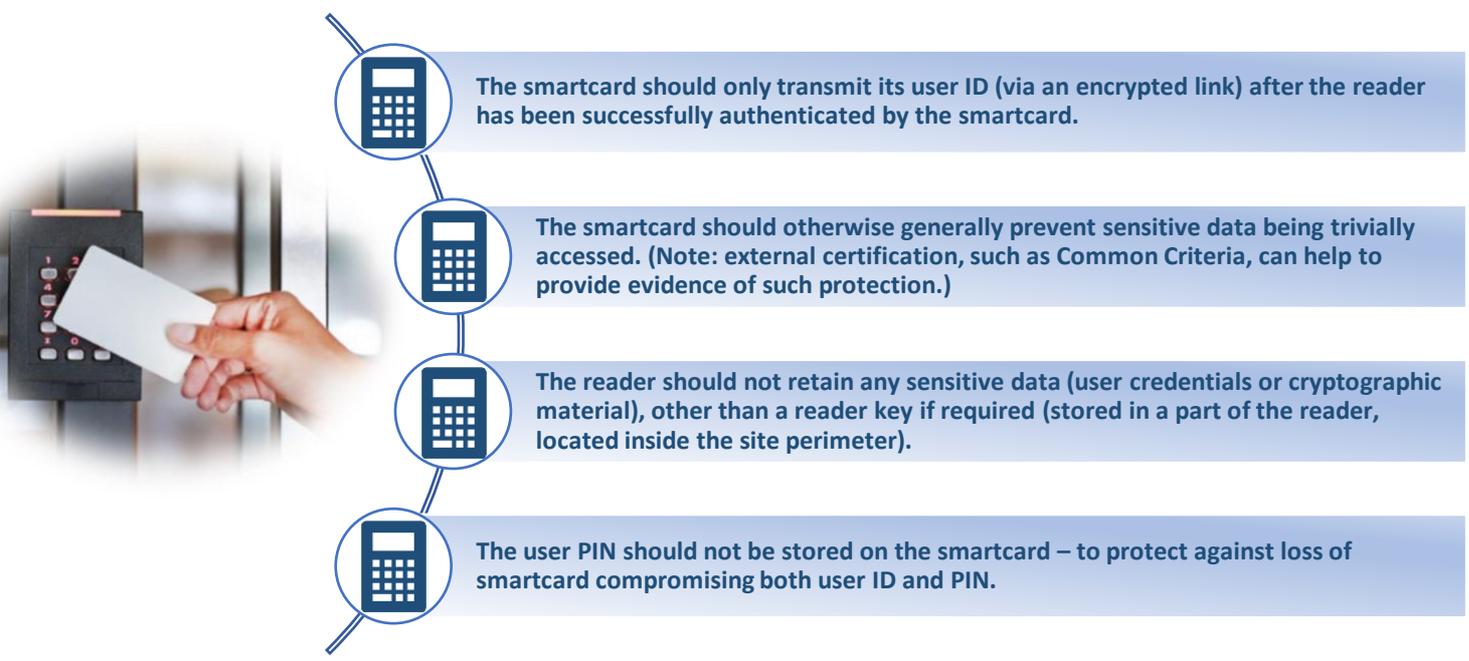
Principal 1 – Protect User ID in Transit

Interception of sensitive data in transit could allow unauthorised site access



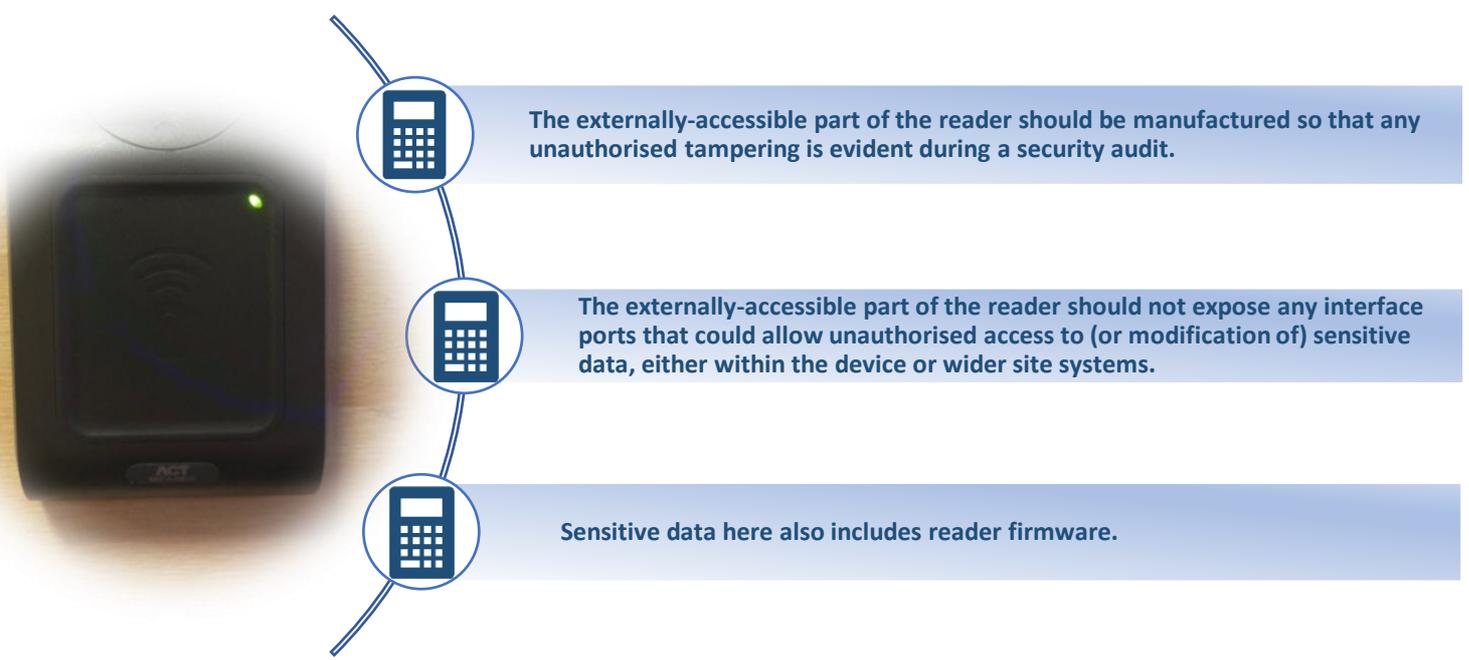
Principal 2 – Protect Sensitive Data at Rest

Unauthorised access to sensitive data on a compromised device could allow unauthorised access



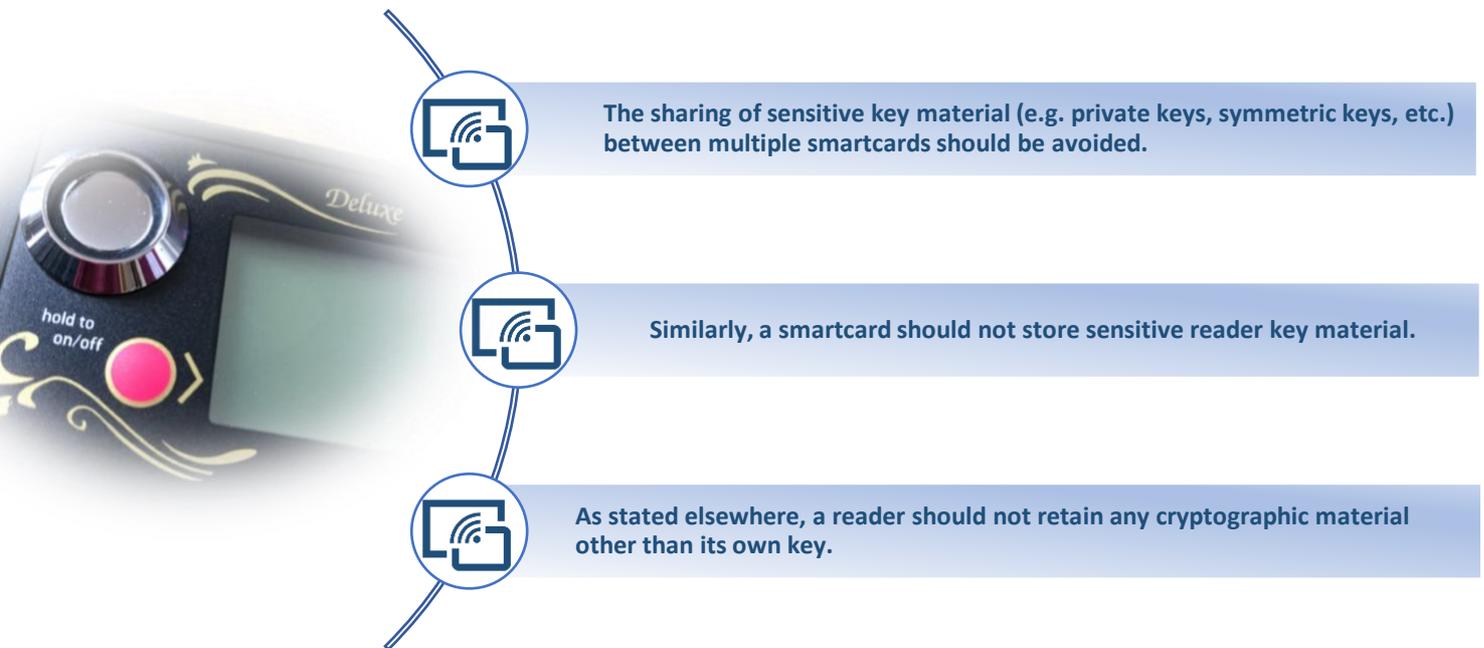
Principal 3 – Externally Accessible Reader Hardware

Undetected reader tampering could allow unauthorised access to user IDs and PINs. Unsecured reader interfaces could allow access to sensitive data.



Principal 4 – Minimise Impact to Compromise

Compromise of smartcards holding cryptographic material shared with other devices could result in wider AACS compromise.



Principal 5 – User Trusted Smartcard Provisioning and Support

Lack of trusted smartcard/PIN management (provisioning, revocation, re-issuing, etc) risks unauthorised persons gaining access to sensitive user access control details.

